



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/931,526	08/16/2001	Arindam Das-Purkayastha	30006636-3	3735

22879 7590 06/19/2008
HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER

CHAI, LONGBIT

ART UNIT	PAPER NUMBER
----------	--------------

2131

NOTIFICATION DATE	DELIVERY MODE
-------------------	---------------

06/19/2008

ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
mkraft@hp.com
ipa.mail@hp.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte ARINDAM DAS-PURKAYASTHA, SIANI LYNNE PEARSON,
and LIQUN CHEN

Appeal 2008-0466
Application 09/931,526¹
Technology Center 2100

Decided: June 17, 2008

Before LANCE LEONARD BARRY, JEAN R. HOMERE, and STEPHEN
C. SIU, *Administrative Patent Judges*.

HOMERE, *Administrative Patent Judge*.

DECISION ON APPEAL
STATEMENT OF THE CASE

¹ Filed on August 16, 2001. The real party in interest is Hewlett Packard Development Co., LP.

Appellants appeal under 35 U.S.C. § 134 from the Examiner's rejection of claims 1 through 61. We have jurisdiction under 35 U.S.C. § 6(b). We affirm-in-part.

The Invention

Appellants invented a method and system for determining the trust level of a computer entity. (Spec. 1.) As depicted in Figure 1, a trusted device (24) computes an integrity metric having values associated with the components of the computer entity (10) by generating a digest of the BIOS instructions in the BIOS memory of the computer entity. (*Id.* 10.) As shown in Figure 3, a controller (30) residing in the trusted device (24) compares the computed values with corresponding measured values for the computer entity to determine the trust levels of the computer entity. (Spec. 9-16.)

Independent claims 1 and 7 further illustrate the invention. They read as follows:

1. Computer apparatus, comprising:

a receiver for receiving an integrity metric for a computer entity via a trusted device associated with the computer entity, the integrity metric having values for a plurality of characteristics associated with the computer entity; and

a controller for assigning a trust level to the computer entity from a plurality of trust levels, wherein the assigned trust level is based upon the value of at least one of the characteristics of the received integrity metric.

7. A method for establishing communications with a computer entity, comprising:

requesting a trusted device associated with a computer entity to provide an integrity metric calculated for the entity by the trusted device and containing values indicative of one or more characteristics of the entity;

receiving a response from the trusted device including an integrity metric calculated for the entity by the trusted device;

comparing values in the integrity metric calculated for the entity by the trusted device with authenticated values provided for the entity by a trusted party; and

selecting a level of trust for the entity from a plurality of predefined levels of trusts based on at least one value in the integrity metric calculated for the entity by the trusted device.

. In rejecting the claims on appeal, the Examiner relies upon the following prior art:

Saunders	US 6,209,099 B1	Mar. 27, 2001
Stoltz	US 6,615,264 B1	Sep. 02, 2003 (filed Apr. 9, 1999)
Grawrock	US 6,678,833 B1	Jan. 13, 2004 (filed Jun. 30, 2000)

The Examiner rejects the claims on appeal as follows:

1. Claims 1 through 9, 11 through 19, 24 through 26, 28 through 37, 40, 42 through 55, and 58 stand rejected under 35 U.S.C. § 102(e) as being anticipated by Grawrock.
2. Claims 10, 27, and 45² stand rejected under 35 U.S.C. § 102(a) as being unpatentable over the combination of Grawrock and Saunders.
3. Claims 20, 21, 38, 39, 41, 56, 57, and 59 stand rejected under 35 U.S.C. § 103 (a) as being unpatentable over the combination of Grawrock and Stoltz.
4. Claims 22, 23, 60, and 61 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Grawrock.

FINDINGS OF FACTS

The following findings of facts (FF) are supported by a preponderance of the evidence.

Grawrock

1. Grawrock discloses a method and system for protecting and accurately reporting boot block data within a computer system by binding a

² We note that the Examiner's statements of the rejection (1 and 2 above) both include claim 45. We note, however, that the claim is only discussed as part of the 103 rejection. (Ans. 12). We therefore treat claim 45 as being rejected under 103, and not 102.

trusted platform module (TPM) to a boot block memory device. (Abstract, col. 2, ll. 1-6.)

2. As depicted in Figure 2, Grawrock discloses a TPM (230) that receives from a boot block memory unit (220) boot information and boot services including boot block code pertaining to the BIOS of the computer system (100) at initialization. (Col. 3, ll. 39-49.)

3. As shown in Figure 3, Grawrock discloses a processor (310) within the TPM that performs a hash operation on the received boot information to produce a boot identifier (330), which is stored in memory (320). (Col. 3, ll. 50-62, col. 4, ll. 1-8.)

4. Grawrock further discloses a challenger that sends a message to the TPM (230) to challenge the integrity of a particular component in the computer system (100). (Col. 4, ll. 9-12.)

5. In response to the challenger's request, the TPM (230) retrieves the corresponding block identifier (330) from memory (320) to provide a digital signature for the requested component. This enables verifying the integrity of the component, and indicating whether the platform is initialized and trusted. (Col. 4, ll. 13-18, ll. 35-37.)

Admitted Prior Art (APA)

6. APA discloses that it is conventional to report integrity metrics and to verify the correctness of the integrity of a computing apparatus by

comparing reported values of metrics with verified values of metrics. (Spec. 1, ll. 21-24.)

PRINCIPLES OF LAW

ANTICIPATION

In rejecting claims under 35 U.S.C. § 102, “[a] single prior art reference that discloses, either expressly or inherently, each limitation of a claim invalidates that claim by anticipation.” *Perricone v. Medicis Pharmaceutical Corp.*, 432 F.3d 1368, 1375 (Fed. Cir. 2005), citing *Minn. Mining & Mfg. Co. v. Johnson & Johnson Orthopaedics, Inc.*, 976 F.2d 1559, 1565 (Fed. Cir. 1992). “Anticipation of a patent claim requires a finding that the claim at issue ‘reads on’ a prior art reference.” *Atlas Powder Co. v. IRECO, Inc.*, 190 F.3d 1342, 1346 (Fed Cir. 1999) (“In other words, if granting patent protection on the disputed claim would allow the patentee to exclude the public from practicing the prior art, then that claim is anticipated, regardless of whether it also covers subject matter not in the prior art.”) (Internal citations omitted).

ANALYSIS

35 U.S.C. § 102

Independent claim 1 recites in relevant part assigning a trust level to a computer entity from a plurality of trust levels based on the value of the characteristics of a received integrity metric. (Claims Appendix A1.)

Appellants argue that Grawrock does not teach the recited limitations. (App. Br. 6-7.) Particularly, Appellants assert that while Grawrock teaches using a boot block identifier to determine whether a computer entity is trusted, it does not teach assigning a trust level to the computer entity based upon a received integrity value. (*Id.* 7.)

The Examiner, in response, finds that Grawrock's disclosure of determining whether a computer entity is trusted or un-trusted based upon the hash values received for the computer components to generate corresponding boot blocks identifiers teaches the claimed invention. (Ans. 16-18.)

Thus, the pivotal issue before us is whether one of ordinary skill in the art would find that Grawrock's use of hash values to determine whether or not a computer entity is trusted teaches assigning a trust level to the computer entity based upon the value of a characteristic of a received integrity metric, as claimed. We answer this inquiry in the affirmative.

We begin by considering the scope and meaning of "integrity metric," which must be given its broadest reasonable interpretation consistent with Appellants' disclosure, as explained in *In re Morris*, 127 F.3d 1048, 1054 (Fed. Cir. 1997):

[T]he PTO applies to the verbiage of the proposed claims the broadest reasonable meaning of the words in their ordinary usage as they would be understood by one of ordinary skill in the art, taking into account whatever enlightenment by way of

definitions or otherwise that may be afforded by the written description contained in the applicant's specification.

Id. at 1054. *See also In re Zletz*, 893 F.2d 319, 321 (Fed. Cir. 1989) (stating that “claims must be interpreted as broadly as their terms reasonably allow.”

Appellants’ Specification states the following:

The trusted device 24 is equipped with at least one method of reliably measuring or acquiring the integrity metric of the computing platform components 10. In the present embodiment, *the integrity metric is acquired by the measurement function 31 by generating a digest of the BIOS instructions in the BIOS memory.* Such an acquired integrity metric, if verified as described above, gives a potential user of the platform 10 a high level of confidence that the platform 10 has not been subverted at a hardware, or BIOS program, level. Other known processes, for example virus checkers, will typically be in place to check that the operating system and application program code has not been subverted.

(Spec. 10.) (Emphasis added.)

Our reviewing court further states, “[t]he ‘ordinary meaning’ of a claim term is its meaning to the ordinary artisan after reading the entire patent.” *Phillips v. AWH Corp.*, 415 F.3d 1303, 1321 (Fed. Cir. 2005).

Upon reviewing Appellants’ Specification, we fail to find any definition of the term “integrity metric” that is different from the ordinary meaning. We find the ordinary meaning of the term “metric” is best found in the dictionary. We note that the definition most suitable for “metric” is

“standard of measurement.”³ We therefore construe the “integrity metric” as a measure of integrity.

As detailed in the Findings of Facts section above, Grawrock discloses that upon receiving boot information from a boot block memory unit, a processor within a TPM performs a hash operation on the received boot information to produce a boot block identifier for a desired computer component, which is stored in memory. (FF. 2-3.) Grawrock further discloses that in response to a challenger’s inquiry request to validate the integrity of the computer entity, the TPM retrieves one or more boot block identifiers from memory to produce a digital signature, which is used to subsequently determine whether or not the computer entity is trusted. (FF. 4-5.) One of ordinary skill in the art would readily recognize that, as correctly pointed out by the Examiner, Grawrock teaches that the computer entity can have one of two trust levels, namely, trusted or un-trusted. (Ans. 17-18.) Further, the ordinarily skilled artisan would aptly recognize that determining which of the trust levels the computer entity possesses depends entirely upon the hash values for the boot block identifiers that the TPM retrieved from the memory to generate the digital signature. Accordingly, the ordinarily skilled artisan would duly appreciate that, by using the values of the boot block identifiers to determine the trust level of the computer entity, Grawrock necessarily teaches assigning a trust level (trusted or un-

³ Webster’s II New Riverside University Dictionary 748 (1994).

trusted) to the computer entity since the nature of such trust level was not known to the challenger and the TPM beforehand. Additionally, the ordinarily skilled artisan would recognize that such trust level is assigned to the computer entity or thereafter determined based upon the values for boot block identifiers of the computer components that are fetched from memory.

“In relying upon the theory of inherency, the Examiner must provide a basis in fact and/or technical reasoning to reasonably support the determination that the allegedly inherent characteristic necessarily flows from the teachings of the applied prior art.” *Ex parte Levy*, 17 USPQ2d 1461, 1464 (Bd. Pat. App. & Inter. 1990). “[A]fter the PTO establishes a prima facie case of anticipation based on inherency, the burden shifts to appellant to ‘prove that the subject matter shown to be in the prior art does not possess the characteristic relied on.’” *In re King*, 801 at 1327(Fed. Cir. 1986) (quoting *In re Swinehart*, 439 F.2d 210, 212-13, (CCPA 1971)). *See also* MPEP §§ 2112 (IV.), (V.).

This reasoning is applicable here. We agree that the Examiner has properly shifted the burden to Appellants by providing a rationale in the Answer that reasonably supports the Examiner’s finding of inherent anticipation with respect to the Grawrock reference. In response, Appellants merely allege that Grawrock’s disclosure does not necessarily teach assigning a trust level to the computer entity based upon a value of a characteristic of a received integrity metric. (App. Br. 16-18, Reply Br. 4-6.) Appellants’ mere allegations are insufficient to prove that the subject

matter shown to be in the prior art does not possess the characteristic relied on by the Examiner. It follows that Appellants have not shown that the Examiner erred in finding that Grawrock anticipates independent claim 1.

Appellants do not provide separate arguments with respect to the rejection of claims 1 through 6, 24 through 26, 28 through 37, and 40. Therefore, we select claim 1 as being representative of the cited claims. Consequently, claims 2 through 6, 24 through 26, 28 through 37, and 40 fall together with representative claim 1. 37 C.F.R. § 41.37(c)(1)(vii).

Regarding independent claim 7, Appellants argue that Grawrock does not teach comparing values for the computer entity calculated by the trusted device with values for the computer entity provided by a trusted party. (App. Br. 8.) We agree with Appellants. The ordinarily skilled artisan would readily recognize that Grawrock teaches at best comparing the values of boot block identifiers calculated by the TPM with corresponding authenticated values provided by the TPM to determine the trust level of the computer entity. (FF. 1-6.) However, we find no teaching in Grawrock indicating that the authenticated values for the computer entity are provided by a trusted party other than the trusted device, as impliedly recited in claim 7. It follows that Appellants have shown that the Examiner erred in finding that Grawrock anticipates independent claim 7. Appellants have similarly shown that the Examiner erred in finding that Grawrock anticipates

independent claim 42, and dependent claims 8, 9, 11 through 19, 43, 44, 46 through 55, and 58 since they also recite the limitation of claim 7 discussed in the preceding paragraph.

35 U.S.C. § 103

Regarding the rejection of claims 27, 38, 39, 41, Appellants argue that these claims are patentable by virtue of their dependency upon independent claim 24, which is allegedly patentable. (App. Br. 9.) Such argument is not persuasive. As discussed above, Appellants have failed to show error in the Examiner's rejection of independent claim 24. It therefore follows that Appellants have failed to show that the Examiner erred in concluding that the combination of Grawrock and Stoltz renders claims 38, 39, and 41 unpatentable. Similarly, Appellants have failed to show that the Examiner erred in concluding that the combination of Grawrock and Saunders renders claim 27 unpatentable.

Regarding the rejection of claims 10, 20 through 23, 45, and 56 through 61, Appellants argue that these claims are patentable by virtue of their dependency upon independent claims 7 and 42, which are patentable. (App. Br. 9.) We agree. As discussed above, Appellants showed error in the Examiner's rejection of claims 7 and 42. Further, we note that neither Stoltz nor Saunders cures the deficiencies that we found in Grawrock. It therefore follows that Appellants have shown that the Examiner erred in concluding

that Grawrock, alone or in combination with either Saunders or Stoltz renders claims 10, 20 through 23, 45, and 56 through 61 unpatentable.

SUMMARY and DECISION

1. Appellants have failed to show that the Examiner erred in:
 - i. finding that Grawrock anticipates claims 1 through 6, 24 through 26, 28 through 37, and 40 under 35 U.S.C. § 102(e).
 - ii. concluding that the combination of Grawrock and Stoltz renders claims 38, 39, and 41 unpatentable under 35 U.S.C. § 103(a).
 - iii. concluding that the combination of Grawrock and Saunders renders claims 27 unpatentable under 35 U.S.C. § 103(a).
2. We therefore affirm these rejections.
3. Appellants have shown that the Examiner erred in:
 - i. finding that Grawrock anticipates claims 7 through 9, 11 through 19, 42 through 44, 46 through 55, and 58 under 35 U.S.C. § 102(e).
 - ii. concluding that the combination of Grawrock and Stoltz renders claims 20, 21, 56, 57, and 59 unpatentable under 35 U.S.C. § 103(a).

Appeal 2008-0466
Application 09/931,526

iii. concluding that the combination of Grawrock and Saunders renders claims 10, and 45 unpatentable under 35 U.S.C. § 103(a).

iv. concluding that Grawrock renders claims 22, 23, 60, and 61 unpatentable under 35 U.S.C. § 103(a).

4. We therefore reverse these rejections.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED-IN-PART

rwk

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS CO 80527-2400